

Use Case

Identity and Access Management

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end solutions that are broadly applicable across a sector, are customizable to the needs of individual businesses, and help businesses more easily comply with relevant standards and regulations.

This document is a detailed description of a particular problem that is relevant across the energy sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the energy sector and vendors of cybersecurity solutions. The solutions proposed by this effort will not be the only ones available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at energy_nccoe@nist.gov.

1. Description

Goal

In order to protect power generation, transmission and distribution, energy companies need to be able to control physical and logical access to their resources, including buildings, equipment, information technology, and supervisory control and data acquisition (SCADA) networks and systems. They need to be able to authenticate the individuals and systems to which they are giving access rights with a high degree of certainty. In addition, energy companies need to be able to enforce access control policies (e.g. allow, deny, inquire further) consistently, uniformly and quickly across all of their resources.

Example Scenario

An energy company technician attempts to enter a substation. She is challenged to prove her identity in a way that provides a high-degree of confidence and is not onerous (e.g., does not require a significant behavior change). Her attempt at entry initiates an authentication request that connects to the company's central authentication service to validate her identity, ensure that she is authorized to access the substation, and confirm that there is a work order on file for that substation and that worker at that time. Once she gains access to the substation, she focuses on the reason for her visit: She needs to diagnose a remote terminal unit (RTU) that has lost its network connectivity. She immediately identifies the cause of the failure as a frayed Ethernet cable and replaces the cable with a spare. She then uses her company-issued mobile device, along with the

Use Case: Identity and Access Management

same electronic credential she used for physical access, to log into the RTU's web interface to test connectivity. The RTU queries the central authentication service to ensure the authenticity and authority of both the technician and her device, then logs the login attempt, the successful authentication and the commands the technician sends during her session.

Background

A foundation of cybersecurity is the principle of least privilege, or the notion that "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."¹ To enforce this principle, the access control system needs to know the appropriate privileges for a given user or system.

Authenticating identity is a necessary step in this process: What a person is allowed to do is based on who that person is. Unfortunately, this requirement is not always met before access is granted.

When a system is compromised, accountability is a necessary part of the subsequent investigation. A security analyst will examine the information exchanges among systems associated with the incident, including which entities made those exchanges. Key to this process is the ability to trace the relevant data behavior based on who (or which system) accessed what, creating a tree of access points.

Successful identity and access management relies on:

- Authentication, authorization and access control requirements on all relevant machines
- Ability to centrally manage the authentication and authorization information for all relevant machines
- Ability to monitor authorized and unauthorized use of all relevant machines
- Authentication, authorization and access control mechanisms that meet business security requirements

2. Security Characteristics

- A single, centrally managed credential for each user or system that can be used throughout the enterprise and operational environments, for both logical and physical access
- Non-intrusive identity and access management capability
- Authentication services that identify a user or system requesting access to a resource
- Authorization and access control services that implement the principle of least privilege

¹ J. Saltzer, Protection and the control of information sharing in multics, *Communications of the ACM*, **17** (7), 388-402 (1974)

Use Case: Identity and Access Management

- 57 • Auditing and monitoring of who did what and when and the ability to share that
- 58 information with a central log analysis tool

59 **3. Business Value**

- 60 • Reduces opportunities for successful attack, as well as the impact of successful
- 61 attacks, thereby lowering overall business risk
- 62 • Increases the probability that investigations of attacks or anomalous system
- 63 behavior will reach successful conclusions
- 64 • Partially satisfies compliance requirements for relevant regulation, thereby
- 65 reducing complexity and cost

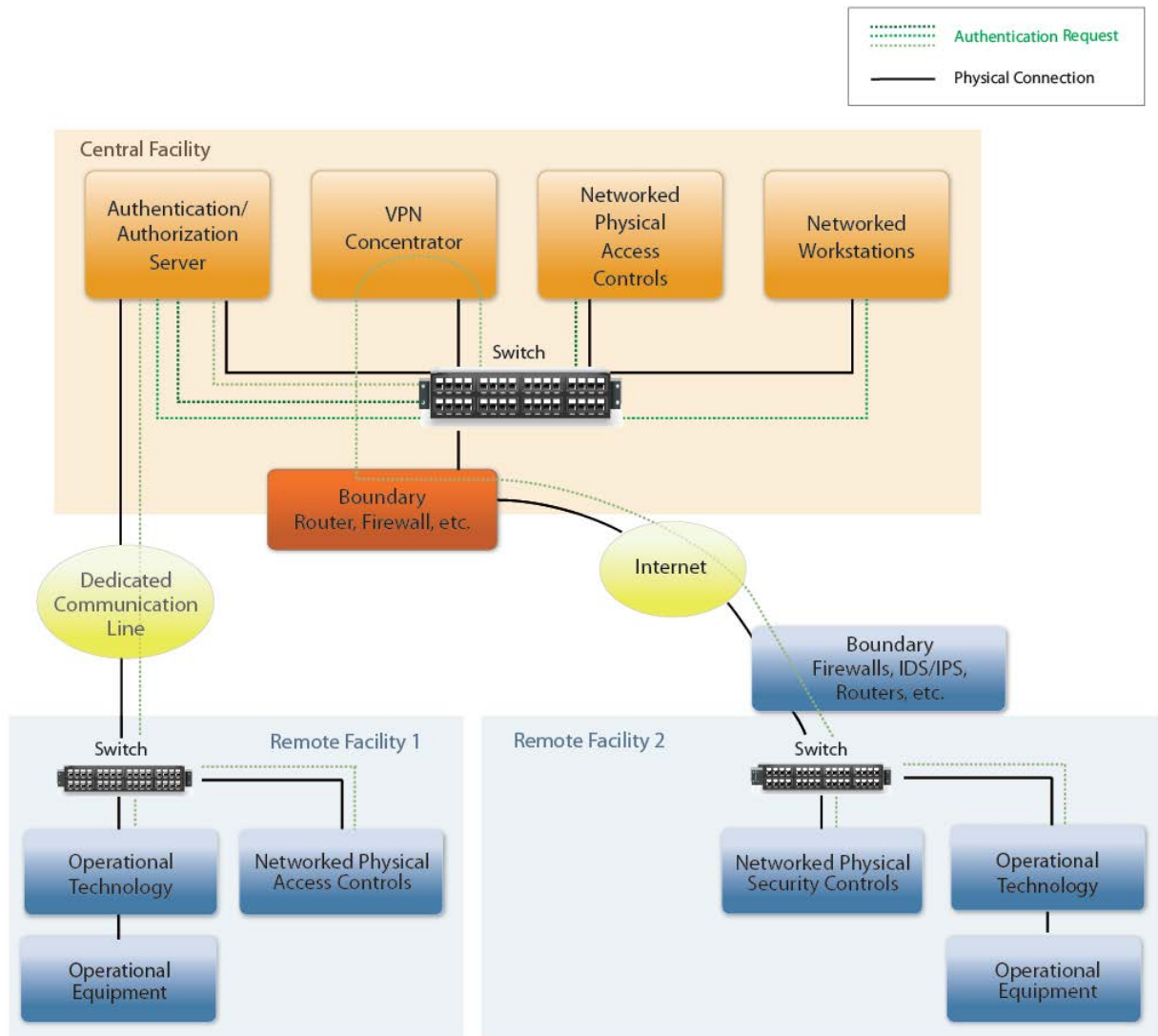
66 **4. Relevant Standards**

- 67 • IEC 62443
- 68 • IEC 62351
- 69 • NERC CIP v.3 and v.5
- 70 • NRC 10 CFR 73.54
- 71 • NRC Regulatory Guide 1.152, Rev. 3
- 72 • NIST IR 7628
- 73 • NIST SP 800-82

74 **5. Component List**

- 75 • Standards-based network
 - 76 ○ Ethernet
 - 77 ○ WiFi
 - 78 ○ Fiber optic
 - 79 ○ Microwave
 - 80 ○ RS-232
- 81 • Enterprise authentication and authorization system for users
- 82 • Enterprise authentication system for devices and software
- 83 • Operational systems (e.g., RTUs, PLCs) that use standard network interfaces and
- 84 are capable of authorizing users against an enterprise authentication/
- 85 authorization system, logging, and controlling logical access
- 86 • Physical access controls with standard network interfaces

87 6. High-Level Architecture



88